Discussion Replies

Name

Institution Affiliation

Discussion Replies

Question One

Discussion 1

Similarities

Discussion one has covered the importance of end-user education in organizations that are susceptible to security breaches. This includes the essentiality of informing employees on the various ways of saving and storing information. This is similar to my findings in that I also agree that the security of systems rely on user habits because hackers explore weak passwords by applying phishing strategies (Snell, 2012). The insight that I have gained from this is that firms should be concerned about training their employees about information security.

Moreover, discussion one discusses the need for encrypted communication in healthcare organizations. The discussion highlights that it is important that messages to any outside source are encrypted. Correspondingly, my findings indicate the need for secure text messaging and encrypted email communication. Healthcare professionals should be able to communicate to each other regarding their patients without exposing confidential data (Snell, 2012). I discovered that lost devices should always have strong encryption to prevent hackers from accessing them.

Differences

The only difference that exists between my findings and that those of discussion one is that it emphasized on the need for companies to provide devices for their staff. Indeed, this will prevent information from passing from a secured network to an unsecured device. However, healthcare companies should focus on encrypting data stored locally on devices. I have learned that this guarantees the safety of patient information from unauthorized access.

Discussion 2

Similarity

Discussion two reports on adverse outcomes of government intervention in cyber security cases. It is true that there are consequences to the state infringing on the privacy of its citizens and exposing systems to hackers in their investigative endeavors. I also found out that the NSA was responsible for the cancellation of Verizon's contract with the German government (Zetter, 2014). What I understood from this was that government surveillance significantly impacts internet security, the integrity of the state's leadership, and the economy.

Difference

Discussion one underlines the effect of government surveillance on companies and the internet but does not show the problem of shortage of cyber security professionals in the country. The Bureau of Labor Statistics reveals that there are less than 89,000 specialists in the U.S (Landi, 2016). This has made me aware of the reason why cyber security experts have the highest salary in the tech field.

Question Two

Discussion 1

Lack of training on cyber security

Inadequately educating employees in healthcare organizations could have grave consequences. For instance, Hollywood Presbyterian Medical Centre experience a loss of $17,000 through paying hackers that seized their patient information (Landi, 2016). Healthcare organizations continue to have difficulty tackling security breaches on their systems.

Discussion 2

Government intrusion in Apple's case

The government requesting Apple to develop code that assists in the investigation of cases has serious effects on the users of Apple devices. This means that many users will have no trust in Apple's automatic updates (Yachot, 2016). Vulnerabilities in Apple devices will remain unsolved, and this will enable a conducive environment for hackers.

Question Three

Discussion 1

Healthcare organizations

There are possible ways through which healthcare providers could reduce the risks that are involved in security breaches. The security divisions of healthcare companies should ensure that they have segmented networks and eliminate default security settings in connected devices. (Landi, 2016). This can go a long way in helping healthcare organizations from experiencing massive losses

Discussion 2

Tech corporations (Apple)

The only way Apple could mitigate the risks posed by government intervention is to refuse the state's request to build a backdoor into their devices. This is because such a breach will allow the government to track one's location, enter into health records, intrude on messages, and access your devices' microphone or camera (Russell, 2016).

Question Four

Discussion 1

Lack of awareness on cyber security in the workforce

A company like Samsung could be potentially affected by having personnel that is unaware of cyber security practices. This would be in the form of loss of its patents through ransomware or intrusion into private company communication. Samsung could eliminate such a risk by ensuring that they provide their employees with simplified training on cyber security knowledge.

Discussion 2

Government surveillance

A home appliance manufacturer like LG can also be affected by backdoors and other types of intrusion that could have an impact on the privacy of their data. The company could mitigate these risks by ensuring that they do not allow the creation of backdoors to their software.

References

Landi, H. (2016). Report: Healthcare industry workers lack basic cyber security awareness. *Healthcare Informatics Magazine*. Retrieved from https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-employees-are-low-hanging-fruit-social-engineering-attacks

Russell, J. (2016). Apple won't create Universal iPhone "Back Door" to aid FBI. Retrieved from https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/

Snell, E. (2012). Why healthcare providers should consider data encryption. Retrieved from https://healthitsecurity.com/news/healthcare-providers-consider-data-encryption

Yachot, N. (2016). 7 reasons a government backdoor to the iPhone would be catastrophic. *American Civil Liberties Union*. Retrieved from https://www.aclu.org/blog/speak-freely/7-reasons-government-backdoor-iphone-would-be-catastrophic

Zetter, K. (2014). Personal privacy is only one of the costs of NSA surveillance. *WIRED*. Retrieved from https://www.wired.com/2014/07/the-big-costs-of-nsa-surveillance-that-no-ones-talking-about/